

Efficient 2-designs from bases exist

Gary McConnell and David Gross

*Institute for Mathematical Sciences, Imperial College London, London SW7 2BW, UK and
QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, UK*

(Dated: February 2, 2008)

We show that in a complex d -dimensional vector space, one can find $O(d)$ bases whose elements form a 2-design. Such vector sets generalize the notion of a maximal collection of mutually unbiased bases (MUBs). MUBs have manifold applications in quantum information theory (e.g. in state tomography, cloning, or cryptography) – however it is suspected that maximal sets exist only in prime-power dimensions. Our construction offers an efficient alternative for general dimensions. The findings are based on a framework recently established in [A. Roy and A. Scott, J. Math. Phys. **48**, 072110 (2007)], which reduces the construction of such bases to the combinatorial problem of finding certain highly nonlinear functions between abelian groups.

I. INTRODUCTION

Two bases $\{|e_i\rangle\}_{i=1,\dots,d}$ and $\{|f_i\rangle\}_{i=1,\dots,d}$ in a d -dimensional Hilbert space are called *mutually unbiased* if $|\langle e_i|f_j\rangle|^2 = 1/d$ for every i, j . It has been shown that there can exist no more than $d + 1$ such bases in \mathbb{C}^d , and, conversely, that this number can be attained whenever d is the power of a prime [2]. It is intuitive that MUBs are advantageous for quantum state tomography, as measurements in unbiased bases reveal “maximally complementary” information about the measured state.

One can make rigorous the intuition that MUBs are “evenly spread out” in state space, by observing that the elements of a maximal collection of MUBs form a *complex projective 2-design* [3, 4, 5, 6, 7]. Roughly speaking, a set of vectors \mathcal{D} is called a t -design, if the average of every t th order polynomial f over the unit sphere in \mathbb{C}^d equals the average of f over \mathcal{D} (see Definition 1 below). Several of the advantageous properties of MUBs follow directly from this feature: e.g. a simple formula for state reconstruction in terms of measurement outcomes or their optimality in certain cloning protocols [1].

A considerable amount of research has gone into the problem of determining $MUB(d)$, the number of MUBs in dimension d [2]. Little is known about $MUB(d)$ when d is not a power of a prime – however, there is some evidence for the fact that $MUB(d) < d + 1$ in these cases [8, 9, 10]. While determining $MUB(d)$ is certainly an important mathematical problem, it may not be the most pertinent question to ask from the point of view of quantum state tomography, as only maximal sets of MUBs can be used for this purpose. So it is timely to look for a “second best” alternative to maximal sets of MUBs.

Therefore, in [1] it was proposed that the problem be approached from a different direction. The authors examine the quantity $M(d)$, defined as the number of bases one needs in dimension d in order to form a 2-design. The number $M(d)$ equals $d + 1$ if and only if there is a complete set of MUBs in d dimensions. In general, $M(d) > d + 1$, but whenever $M(d)$ is reasonably small, such sets of bases can serve as a good substitute for MUBs [1]. We call a 2-design of this kind *efficient* if it consists of $O(d)$ bases.

It was shown in [1] that $M(d) \leq \frac{3}{4}(d - 1)^2$. Here, we improve their results by constructing weighted complex projective 2-designs from roughly $2(d + \sqrt{d})$ bases for odd d and $3(d + \sqrt{d})$ bases in even dimensions.

II. DEFINITIONS AND PREVIOUS RESULTS

Let f be a homogeneous polynomial of order t in $2d$ variables. We can regard f as a function on \mathbb{C}^d by evaluating it on coordinates (with respect to an arbitrary fixed basis) and their complex conjugates: $f(|\psi\rangle) = f(\psi_1, \dots, \psi_d; \bar{\psi}_1, \dots, \bar{\psi}_d)$. The set of such polynomials is denoted by $\text{Hom}(t, t)$.

Definition 1 (Weighted 2-designs). *Let \mathcal{D} be a set of normalized vectors in \mathbb{C}^d and $w : \mathcal{D} \rightarrow [0, 1]$ a normalized weight function. The set \mathcal{D} together with the weights w is a weighted complex projective 2-design if for all $f \in \text{Hom}(2, 2)$ the relation*

$$\sum_{x \in \mathcal{D}} w(x) f(x) = \int_{\mathbb{C}P^{d-1}} f(x) dx \quad (1)$$

holds.

The integral on the right hand side of (1) is understood to be taken with respect to the Haar measure on $\mathbb{C}P^{d-1}$. We will make use of a combinatorial construction for weighted 2-designs introduced in [1]. To this end:

Definition 2 (Differential 1-uniformity [1]). *Let A, B be finite abelian groups. The function $f : A \rightarrow B$ is differentially 1-uniform ($d1u$) if the equation*

$$f(x + a) - f(x) = b \quad (2)$$

has at most one solution in x for every $(a, b) \neq (0, 0)$.

Differentially 1-uniform functions are related to *highly non-linear functions*, which have been the subject of research in combinatorics and cryptography [12].

Theorem 3 (2-designs from d1u functions [1]). *If $f : A \rightarrow B$ is d1u, then there is a weighted complex projective 2-design formed from $|B| + 1$ bases in dimension $d = |A|$.*

Hence the challenge is to construct d1u functions from general A to some B which is as small as possible. Our particular construction below makes use of d1u functions with *cyclic domain* $A = \mathbb{Z}/d\mathbb{Z}$.

For any positive integer d , denote by $\mathbf{C}(d)$ the smallest cardinality of an abelian group B such that there exists a d1u function $f : \mathbb{Z}/d\mathbb{Z} \rightarrow B$. The following theorem summarizes the relevant results of [1].

Theorem 4 (Known bounds on $\mathbf{C}(d)$ [1]). *With notation as above:*

1. *If d is an odd prime power, then $\mathbf{C}(d) = d$ (which is optimal).*
2. *For $d = p^k - 1$, where p is an arbitrary prime number and k is any positive integer, we have $\mathbf{C}(d) \leq d + 1$.*
3. *For general d , $\mathbf{C}(d) \leq \frac{3}{4}(d - 1)^2$.*

III. AN $O(d)$ BOUND FOR $\mathbf{C}(d)$

We aim to improve the bounds of Theorem 4. The essence of the result is that $\mathbf{C}(d)$ is linear in d :

Theorem 5. $\mathbf{C}(d) = O(d)$.

More precisely, let d be any integer ≥ 2 . Let q_d denote the smallest integer $\geq d - 1$ such that there exists a d1u function $\mathbb{Z}/q_d\mathbb{Z} \rightarrow B$ whose codomain B is of minimal order $|B| = \mathbf{C}(q_d)$, among all such integers and d1u functions.

For example, if $d - 1$ is an odd prime, then by Theorem 4 we can take $q_d = d - 1$, $B = \mathbb{Z}/q\mathbb{Z}$ and clearly then $|B| = q$ will be minimal.

The key result of this paper is as follows.

Theorem 6. *Let d be any integer ≥ 2 and define q_d as above.*

1. *If d is odd then $\mathbf{C}(d) \leq 2\mathbf{C}(q_d)$;*
2. *and if d is even, $\mathbf{C}(d) \leq 3\mathbf{C}(q_d)$.*

By taking q_d to be the smallest prime greater than or equal to d , we get the following explicit asymptotic bounds:

Corollary 7. *Let d be as above and let $\theta = 0.525$ [13]. For d large enough, we have that*

1. *for d odd, $\mathbf{C}(d) \leq 2(d + d^\theta)$;*
2. *and similarly for d even, $\mathbf{C}(d) \leq 3(d + d^\theta)$.*

We prove these results by constructing explicit functions from $\mathbb{Z}/d\mathbb{Z}$ into groups of the sizes shown.

A. Differentials and group homomorphisms

Let A, B be two arbitrary finite abelian groups, written additively. We shall assume that $|B| \geq |A| \geq 2$. Let $\mathbf{Map}(A, B)$ denote the set of all functions between A and B , which itself is a finite abelian group under pointwise addition.

Given any $a \in A$ and $f : A \rightarrow B$, define the differential operator $D_a : \mathbf{Map}(A, B) \rightarrow \mathbf{Map}(A, B)$ by

$$D_a(f)(x) = f(a + x) - f(x),$$

for any x in A . In this terminology, Definition 2 may be rephrased thus: the function f is d1u if for all non-zero $a \in A$, the vector $(D_a(f)(x))$ contains no repeated values (here we fix an ordering of the elements $x \in A$). This makes precise the somewhat loose notion that f is d1u if it is as “far from being a homomorphism as possible”. Indeed, yet another equivalent formulation of the condition that a function f be d1u is that its second differentials $D_{a_1}D_{a_2}f$ be nowhere-vanishing for all $a_1, a_2 \in A \setminus \{0\}$.

There is a symmetry relation among the vectors $D_a(f)$ of differentials which follows from the identity:

$$D_a(f)(x) = -D_{-a}(f)(a+x), \quad (3)$$

for all $a, x \in A$. As a practical matter therefore, to check if a function f is d1u, it suffices to check “the first half” of the vectors $D_a(f)$. In addition, the following useful identity holds:

$$D_{ra}(f)(x) = \sum_{i=0}^{r-1} D_a(f)(ia+x), \quad (4)$$

for all $r \in \mathbb{Z}$, $x \in A$ and for all nonzero $a \in A$. If A is cyclic then each vector $D_a f$ is easily determined using (4) from the one generating vector $D_1 f$. This obviously also holds within the cyclic subgroups of a general abelian group A .

B. The construction

We now present a new class of d1u functions which improves the bound in (3) of Theorem 4. Henceforth we assume $A = \mathbb{Z}/d\mathbb{Z}$. The aim is to find n as small as possible such that there exists a group B of order n and a d1u function $f : A \rightarrow B$.

So let d be any integer ≥ 2 . Let p be the least prime which is coprime to d . Let q be any integer $\geq d-1$ such that there exists a finite abelian group G and a d1u function $\phi : \mathbb{Z}/q\mathbb{Z} \rightarrow G$. For example, by Theorem 4 we may take q to be any odd prime $\pi \geq d-1$, or else $q = \pi^k + 1$ for π any prime, $k \geq 1$ (see [1] §4 for the actual functions ϕ in this case).

We write ϕ_d for the ‘restriction’ of ϕ to $\mathbb{Z}/d\mathbb{Z}$, viz.:

$$\phi_d(x) = \phi(x), \quad 0 \leq x \leq d-1,$$

where it is understood that ϕ_d is defined modulo d and where we set $\phi_d(d-1) = \phi(q) = \phi(0)$ in the case $q = d-1$.

Then we are able to construct examples of d1u functions as follows. We are grateful to Aidan Roy for pointing out the neat form in which our original (less general) construction has been rephrased below.

Proposition 8. *Let d, p, q, G, ϕ_d be as above. Define $f : \mathbb{Z}/d\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times G$ by*

$$f(i) = (i, \phi_d(i)), \quad (5)$$

for $0 \leq i \leq d-1$. Then f is d1u.

Proof. Case (i): $q \geq d$. Fix $a \in \mathbb{Z}/d\mathbb{Z}$. Observe that for every $x \in \mathbb{Z}/d\mathbb{Z}$ with $0 \leq a+x \leq d-1$:

$$D_a \phi_d(x) = \phi_d(a+x) - \phi_d(x) = \phi(a+x) - \phi(x) = D_a \phi(x),$$

(where we always write a and x as the smallest positive integers representing their respective congruence classes modulo d or q as the case may be). Since ϕ is d1u, we know therefore that the values $D_a \phi_d(x)$ are distinct in G as x runs from 0 to $d-1-a$. Hence the same must be true of the $D_a f(x)$ for such x because of the identity

$$D_a f(x) = (D_a(x), D_a \phi_d(x)).$$

Remark 9. *Note that one must take some care with this function $D_a(x)$ when $a+x \geq d$: the shift function $x \mapsto a+x$ operates modulo d (not q) and so in fact the congruence class of $a+x$ is $a+x-d$ for the purposes of evaluating these differentials. For $0 \leq x \leq d-1-a$ there is no ambiguity and $D_a(x)$ is just equal to a .*

So it remains to show that the values of $D_a f(x)$ for $d-a \leq x \leq d-1$ are distinct from one another, and that they do not coincide with any of the values just described for $0 \leq x \leq d-1-a$. This latter point follows from the remark above, since p is coprime to d and so for $a+x \geq d$:

$$D_a(x) = a+x-d-x = a-d \not\equiv a \pmod{p}.$$

We have reduced the problem to the assertion that for $d-a \leq x \leq d-1$, the $D_a \phi_d(x)$ are distinct. But it follows from the definitions of ϕ and ϕ_d that

$$D_a \phi_d(x) = \phi_d(a+x) - \phi_d(x) = \phi(a+x+q-d) - \phi(x) = D_{a+q-d} \phi(x),$$

which again by the choice of ϕ as a d1u function, cannot have repeated values inside G .

Case (ii): $q = d - 1$. The proof is almost identical to that for case (i), the only added complication being that one has to consider the value

$$D_a \phi_d(d - 1 - a) = \phi_d(d - 1) - \phi_d(d - 1 - a) = \phi(0) - \phi(q - a)$$

which arises when $x = d - 1 - a (= q - a)$, and to show that it does not already exist in the set of $D_a \phi(x)$ for $0 \leq x \leq q - a - 1$. But

$$\phi(0) - \phi(q - a) = D_a \phi(q - a),$$

which by the fact that ϕ is dlu cannot lie in the set described. \square

So for odd d , we can choose q to be prime and employ Theorem 4 to obtain an upper bound for $C(d)$ of twice the smallest prime $\geq d - 1$. By Chebyshev's theorem, there is always a prime between d and $2d$, so $C(d) \leq 4d$. Making use of more elaborate bounds on the worst case gap between two consecutive primes [13], we obtain the result advertised in Corollary 7.

However, for even d we are constrained to around $3d$ at best; and for dimensions where d is divisible by 3×2 , it is often much worse. For example if $d = 30030$, then the best bound given by this construction is $30029 \times 17 = 510510$. So we now provide a tighter bound for even values of d .

Proposition 10. *Let d, q, G, ϕ, ϕ_d be as above, with d even. Let a 'flag' function $\theta : \mathbb{Z}/d\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$ be defined by $\theta(x) = 0$ for $0 \leq x \leq d/2 - 1$ and $\theta(x) = 1$ for $d/2 \leq x \leq d - 1$. Then*

$$f : \mathbb{Z}/d\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \times G : f(i) = (\theta(i), \phi_d(i)) \quad (6)$$

is dlu.

Proof. It is clear from the structure of the function f that we may rely almost completely upon the previous proof, bearing in mind Remark 9. By equation 3 we need only focus on a in the range $1 \leq a \leq d/2$. Then all we need to observe is that in 'crossing the $a + x = d$ threshold', the functions $D_a f$ switch their flag $D_a \theta(x)$ to -1 from 0 (or from $+1$ for $d/2 - a \leq x \leq d/2 - 1$), hence ensuring that the sets

$$D_a f(x), 0 \leq x \leq d - 1 - a$$

and

$$D_a f(y) = (-1, D_{a+q-d} \phi(y)), d - a \leq y \leq d - 1$$

remain disjoint. Note that a similar observation to the one in Proposition 8 takes care of the case $q = d - 1$. \square

This ends the proof of Theorem 6, and by extension of Theorem 5.

IV. COMPUTER FINDINGS IN LOW DIMENSIONS

The results presented above give solutions which are within a multiplicative constant of the theoretical optimum $C(d) = d$. Still, computer searches reveal that better dlu functions are very likely to exist in general – at least whenever d is neither an odd prime power nor of the form $p^k - 1$ for prime p . The first three numbers which are not of this form are $d = 14, 20$ and 21 . The table below compares recent computer findings of Andrew Scott (private communication) in these dimensions, with the systematic methods of the present note.

d	14	20	21
Systematic: $C(d) \leq$	39	57	46
Computer: $C(d) \leq$	20	32	37

(7)

Scott has further shown by exhaustive search methods that no dlu function exists from $\mathbb{Z}/14\mathbb{Z}$ into any abelian group of order less than 20.

V. ACKNOWLEDGMENTS

We would like to thank Andrew Scott and Aidan Roy for their help in orienting this work and Terry Rudolph for many thought-provoking conversations.

This work has been supported by QAP, the EURI Award of J. Eisert, and the QIP-IRC.

-
- [1] A. Roy, A. Scott, J. Math. Phys. **48**, 072110 (2007).
 - [2] W.K. Wootters and B.C. Fields, Ann. Phys. **16**, 391 (1989); S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica, **34**, 512 (2002); S. Chaturvedi, Phys. Rev. A **65** 0044301 (2002).
 - [3] P. Delsarte, J. Goethals, J. Seidel, Geom. Dedicata **6**, 363 (1977).
 - [4] H. König, *Cubature formulas on spheres*, Advances in multivariate approximation (Witten-Bommerholz, 1998), Math. Res., **107**, Wiley-VCH, Berlin (1999).
 - [5] A. Klappenecker and M. Rötteler, Proceedings of the IEEE International Symposium on Information Theory, 1740 (2005).
 - [6] C. Dankert, R. Cleve, J. Emerson, E. Livine, quant-ph/0606161 (2006); D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48**, 052104 (2007).
 - [7] A. Ambainis and J. Emerson, Computational Complexity 2007, quant-ph/0701126.
 - [8] C. Archer, quant-ph/312204 (2003).
 - [9] M. Grassl, quant-ph/0406175 (2004).
 - [10] M. Aschbacher, A. Childs, and P. Wocjan, Journal of Algebraic Combinatorics, **25**, 111 (2007).
 - [11] I. Bengtsson, W. Bruzda, A. Ericsson, J.-A. Larsson, W. Tadej, and K. Zyczkowski, J. Math. Phys. **48**, 052106 (2007).
 - [12] C. Carlet and C. Ding, Journal of Complexity **20**, 205 (2004).
 - [13] R. Baker, G. Harman, and J. Pintz, Proc. London Math. Soc. **83**, 532 (2001).